University of Bahrain
College of Information Technology
Department of Computer Science
First Semester, 2013-2014
ITCS412 (Cryptography and Network Security)

Test I

Duration: One Hour

Time: 3:00PM - 4:00PM

STUDENT NAME	
STUDENT ID #	
SECTION #	9:00 → 12:00 →

NOTE: THERE ARE SIX (6) **PAGES** IN THIS TEST
ONLY ONE SOLUTION WILL BE CONSIDERED FOR EACH QUESTION

Part #	MARKS		COMMENTS
1	10	10	
2	20	17½	
3	10	8	
TOTAL	40	35½	

DRAGON

Part 1:

Answer the following questions by clearly circling *the most appropriate* answer (1 point each)

1. Implements the security *policies* of the data processing systems and information transfers of an organization

   a. Security service
   b. Security architecture
   c. Security attack
   d. Security mechanism

2. Access Control mechanism

   a. Ensures the identity of an entity
   b. Enforces access rights to resources
   c. Enhances detection of security relevant events
   d. Enables the selection of particular physical secure route

3. A person in possession of a sample of ciphertext and corresponding plaintext is capable of what type of attack?

   a. Ciphertext only
   b. Chosen-plaintext
   c. Known-plaintext
   d. Plaintext only

4. What type of cryptanalytic attack where an adversary has the least amount of information to work with?

   a. Known-plaintext
   b. Ciphertext-only
   c. Plaintext-only
   d. Chosen-ciphertext

5. What encryption operation is used when AES uses S-boxes during the process of encryption?

   a. Chaining
   b. Key exchange
   c. Key generation
   d. Substitution

6. Which of the following encryption methods is considered unbreakable?

   a. One-time pads
   b. DES codebooks
   c. Symmetric ciphers
   d. Elliptic-curve cryptography

7. If block size is *n* and *n* is big, then we need $2 \times n \times 2^n$ table for key. Which is a big table, a good solution to reduce key size would be

   a. Use alternating sequence of substitutions and permutations
   b. Approximate random mapping by components controlled by the key
   c. Process block using key to produce output that is diffuse and confused.
   d. Use two or more ciphers as simple encryption operations with same key done repeatedly

8. What is the main component in a Feistel network that is responsible for diffusion

   a. The S-box
   b. The subkeys
   c. The swap operation
   d. The initial permutation (IP)

9. DES creates 16 subkeys from a key. Which of the following can be considered a weak key:

   a. Weak keys: keys with more ones than zeros
   b. Weak keys: keys with more zeros than ones.
   c. Weak keys: keys that make all subkeys to be different.
   d. Weak keys: keys make the same subkey to be generated in more than one round.

10. In cryptography, a strong encryption algorithm assumes that if an attacker knows the plaintext and the ciphertext, it is still infeasible for him to know the key. This assumption is based on the concept of,

    a. Feistel
    b. Diffusion
    c. Confusion
    d. avalanche

Part 2:

1. List one passive attack and one active attack. [2 points]

2 - passive attack: packet analyzing
- active attack: capturing data and modify it the send it.

2. Why playfair algorithm is better than mono-alphabet? [2 points]

2 because playfair uses 26x26 set of alphabetic which is way more than mono-alphabet (26), and this make recognizing language characteristic much harder.

3. Playfair and polyalphabet algorithms both use a keyword. However, polyalphabet is considered better than playfair. Why? [2 points]

2 because playfair show some language characteristic, because every two letters will be matched to the exact two letters every time, but in polyalphabet there is a great chance that ever letter will be matched with different letter each time.

4. How to improve block ciphers? List two [2 points]

- diffusion
- confusion ✗

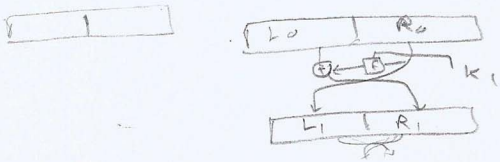
5. Construct a playfair matrix with the key ***Techno*** and encrypt the following message ***Generaly***.

[4 points]

t	e	c	h	n
o	a	b	d	f
g	i/j	k	l	m
p	q	r	s	u
v	w	x	y	z

generaly
- ittcqbhs
or - jttcqbhs
sh

4



6. Given the following symbols used in DES {L_0, R_0, F, XOR, L_1, R_1, K_1} [4 points]

i. Write the encryption equations to produce L_1 and R_1 for one round of DES from L_0 and R_0

$L_1 = R_0$

$R_1 = L_0 \oplus F(R_0, K_1)$

ii. Write the decryption equations to produce L_0 and R_0 from L_1 and R_1 calculated in (a) and prove the equality.

$L_0 = L_1 = R_0$

$R_0 = R_1 \oplus F(L_1, K_1)$

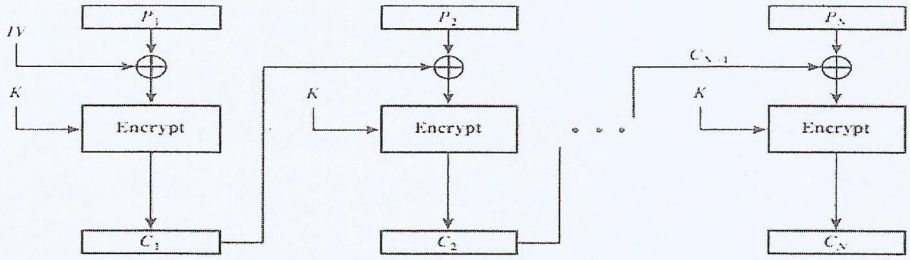
$L_0 \oplus F(R_0, K_1) \rightarrow R_0 \Rightarrow$

$R_0 = L_0 \oplus F(R_0, K_1) \oplus F(R_0, K_1)$

$R_0 = L_0 \oplus 0$

$R_0 = L_0 = R_1$

7. Answer the following questions relating to modes of operation. [4 points]



(a) Encryption

a. What is the name of the mode of operation illustrated in the above diagram.

cipher block chaining (CBC)

b. List one advantage

- blocks are dependent on each other

c. List two limitations

- error propagation
- must have IV with the sender and reciever.

Part 3:

1. Why DES has 16 rounds? explain [2 points]

to achive avalanch effect.

2. What improvement does 3DES exhibit over DES? [1 point]

much bigger key size, and hence it is harder to brute force.

3. Why 3DES performs E-D-E and not E-E-E ? (E for Encryption, D for Decryption) [1 points]

because encryption is equivelent to decryption, and if we use only one key, it will be backward compatable with DES.

4. The S-box is a permutation of all 256-bit values and therefore it is fixed. What it is the main criteria in the design of S-box values. [1 points]

to provide subtitution of data (confusion), it should make it hard to obtain the key.

5. One round of AES consists of four main operations: [1 points]
ByteSub, ShiftRow, MixColumn and AddRoundKey.

How AES performs Decryption for the above operations?
- Addroundkey: using it in the reverse order
- MixColumn: multiplay by invers matrix
- shiftRow: shift to righ.
- ByteSub: the inverse.

6. In DES, encryption function is the same as decryption function. In AES decryption is different than encryption. Explain what modifications are needed to make AES decryption function similar to encryption function. [2 points]

we can rearrange the operations, because "ByteSub" and "ShiftRow" are reversable, and also "Mix Column" and "AddRoundkey".

7. Is AES a Fiestel Cipher? Why? [1 point]

No, it is iterative.

8. Explain why in one-time pad algorithm repeating the key is not secure. [1 point]

because if we have two ciphers, it will be easy to recover the key and plaintext